AMENDMENTS TO THE CLAIMS

1-8. (Cancelled)

9. (Currently Amended) A method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the ~~plurality of~~ associated encryption keys ~~to generate a plurality of digital object ciphertexts~~;

encrypting the plurality of encryption keys using a first cryptography scheme ~~key to generate a plurality of encryption key ciphertexts~~;

transmitting to a requester the plurality of encrypted digital objects ~~ciphertexts~~ and encryption keys ~~ciphertexts~~;

receiving from the requester ~~an~~ at least one of the encryption keys, wherein the received encryption key has been ~~ciphertext~~ further encrypted using a second cryptography scheme ~~key~~;

generating a partially decrypted encryption key by decrypting the received encryption key ~~ciphertext~~ using the first cryptography scheme ~~key to generate a partially decrypted encryption key~~; and

transmitting the partially decrypted encryption key to the requester.

10. (Previously Presented) The method of claim 9, further comprising encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

11. (Currently Amended) The method of claim 9, further comprising decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))} \bmod$ (prime number p).

12. (Currently Amended) The method of claim 10, further comprising performing the modulo operation if computation of a discrete logarithm is ~~infeasible~~ not possible.

13. (Currently Amended) A method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested [[a]] plurality of ~~ciphertext~~ digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the [[a]] plurality of ~~ciphertext~~ keys associated with the plurality of ~~ciphertext~~ digital objects wherein each key has been encrypted using a first cryptography scheme;

selecting a ~~ciphertext~~ key from the plurality of received ~~ciphertext~~ keys;

further encrypting the selected ~~ciphertext~~ key using a second cryptography scheme ~~first key to generate a further encrypted ciphertext key~~;

transmitting the ~~further encrypted ciphertext~~ key to the database;

receiving from the database ~~a ciphertext~~ the key wherein the key has been partially decrypted using the first cryptography scheme ~~a second key~~;

decrypting the partially decrypted ~~ciphertext~~ key using the second cryptography scheme ~~first key~~ to generate a decrypted key; and

decrypting the received ~~ciphertext~~ digital object using the decrypted key.

14. (Previously Presented) The method of claim 13, further comprising encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

15. (Currently Amended) The method of claim 13, further comprising decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p).

16. (Currently Amended) The method of claim 14, further comprising performing the modulo operation if computation of a discrete logarithm is ~~infeasible~~ not possible.

17. (Currently Amended) A system for selecting a digital object in a database, the system comprising a processor for:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the ~~plurality of~~ associated encryption keys ~~to generate a plurality of digital object ciphertexts~~;

encrypting the plurality of encryption keys using a first ~~key to generate a plurality of encryption key ciphertexts~~ cryptography scheme;

transmitting to a requester the plurality of encrypted digital ~~object ciphertexts~~ objects and encryption ~~key ciphertexts~~ keys;

receiving from the requester ~~an~~ at least one of the encryption keys, wherein the received encryption key has been ~~ciphertext~~ further encrypted using a second ~~key~~ cryptography scheme;

generating a partially decrypted encryption key by decrypting the received encryption key ~~ciphertext~~ using the first ~~key to generate a partially decrypted encryption key~~ cryptography scheme; and

transmitting the partially decrypted encryption key to the requester.

18. (Previously Presented) The system of claim 17, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

19. (Currently Amended) The system of claim 17, wherein the processor is further configured or arranged for decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p).

20. (Currently Amended) The system of claim 18, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is ~~infeasible~~ not possible.

21. (Currently Amended) A system for selecting a digital object in a database, the system comprising a processor for:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested [[a]] plurality of ~~ciphertext~~ digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the [[a]] plurality of ~~ciphertext~~ keys associated with the plurality of ~~ciphertext~~ digital objects wherein each key has been encrypted using a first cryptography scheme;

selecting a ~~ciphertext~~ key from the plurality of received ~~ciphertext~~ keys;

further encrypting the selected ~~ciphertext~~ key using a second cryptography scheme ~~first key to generate a further encrypted ciphertext key~~;

transmitting the ~~further encrypted ciphertext~~ key to the database;

receiving from the database ~~a ciphertext~~ the key wherein the key has been partially decrypted using the first cryptography scheme ~~a second key~~;

decrypting the partially decrypted ~~ciphertext~~ key using the second cryptography scheme ~~first key~~ to generate a decrypted key; and

decrypting the received ~~ciphertext~~ digital object using the decrypted key.

22. (Previously Presented) The system of claim 21, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

23. (Currently Amended) The system of claim 21, wherein the processor is further configured or arranged for decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p).

24. (Currently Amended) The system of claim 22, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is ~~infeasible~~ not possible.

25. (Currently Amended) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the ~~plurality of~~ associated encryption keys ~~to generate a plurality of digital object ciphertexts~~;

encrypting the plurality of encryption keys using a first cryptography scheme ~~key to generate a plurality of encryption key ciphertexts~~;

transmitting to a requester the plurality of encrypted digital ~~object~~ ~~ciphertexts~~ objects and encryption ~~key~~ ~~ciphertexts~~ keys;

receiving from the requester ~~an~~ at least one of the encryption keys, wherein the received encryption key has been ~~ciphertext~~ further encrypted using a second ~~key~~ cryptography scheme ;

generating a partially decrypted encryption key by decrypting the received encryption key ~~ciphertext~~ using the first ~~key to generate a partially decrypted encryption key~~ cryptography scheme; and

transmitting the partially decrypted encryption key to the requester.

26. (Previously Presented) The machine-readable medium of claim 25, wherein the method further comprises encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

27. (Currently Amended) The machine-readable medium of claim 25, wherein the method further comprises decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p).

28. (Currently Amended) The machine-readable medium of claim 26, wherein the modulo operation is performed if computation of a discrete logarithm is ~~infeasible~~ not possible.

29. (Currently Amended) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested [[a]] plurality of ~~ciphertext~~ digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the [[a]] plurality of ~~ciphertext~~ keys associated with the plurality of ~~ciphertext~~ digital objects wherein each key has been encrypted using a first cryptography scheme;

selecting a ~~ciphertext~~ key from the plurality of received ~~ciphertext~~ keys;

further encrypting the selected ~~ciphertext~~ key using a second cryptography scheme ~~first key to generate a further encrypted ciphertext key~~;

transmitting the ~~further encrypted ciphertext~~ key to the database;

receiving from the database ~~a ciphertext~~ the key wherein the key has been partially decrypted using the first cryptography scheme ~~a second key~~;

decrypting the partially decrypted ~~ciphertext~~ key using the second cryptography scheme ~~first key~~ to generate a decrypted key; and

decrypting the received ~~ciphertext~~ digital object using the decrypted key.

30. (Previously Presented) The machine-readable medium of claim 29, wherein the method further comprises encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

31. (Currently Amended) The machine-readable medium of claim 29, wherein the method further comprises decrypting the received encryption key ~~ciphertext~~ by determining (encryption key ~~ciphertext~~)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p).

32. (Currently Amended) The machine-readable medium of claim 27, wherein the method further comprises performing the modulo operation if computation of a discrete logarithm is ~~infeasible~~ not possible.